ON THE CONSTRUCTION OF HADAMARD MATRICES (Algebraic Combinatorics)

Baylon, Rowena T.

数理解析研究所講究録 1394 巻 2004 年 88-96

ON THE CONSTRUCTION OF HADAMARD MATRICES

ROWENA T. BAYLON†
KYUSHU UNIVERSITY
GRADUATE SCHOOL OF MATHEMATICS 33
FUKUOKA 812-8581
JAPAN
EMAIL: BAYLON@MATH.KYUSHU-U.AC.JP

ABSTRACT. This paper constructs Hadamard matrices of order $4n$. Given the first 4 rows and columns of a Hadamard matrix of order $4n$, we study its $(n-1)\times(n-1)$ block matrix properties. Since the incidence matrices of symmetric 2-designs do not violate the obtained properties, we use them in the construction. We obtained the total number of Hadamard matrix construction structures by only using incidence matrices of symmetric 2-designs. Furthermore, at most 4 different incidence matrices with their corresponding complements can have a Hadamard matrix structure. Other than this number is not possible.

1. INTRODUCTION

A *Hadamard matrix* of order n is a square matrix H whose entries consist of 1's and -1's satisfying

$$HH^T = nI$$

where H^T is the transpose of H and I is the identity matrix of order n. It is known that Hadamard matrices exist only when $n=2$ or n is a multiple of 4. However, the converse still remains as a conjecture at present[11]. In particular, for $n \leq 28$, Hadamard matrices are completely classified and the complete listing of such matrices can be found in Sloane's homepage[14]. This paper aims to construct Hadamard matrices of order $4n$ by investigating Kimura's structure [9] for length 32. We determine the appropriate parameters of all the

Date: March 29, 2004.
†This work is (partially) supported by Kyushu University 21st Century COE Program, Development of Dynamic Mathematics with High Functionality, of the Ministry of Education, Culture, Sports, Science and Technology of Japan.

submatrices, having order $n-1$, that will yield a Hadamard matrix of order $4n$. It is seen that the appropriate choice of incidence matrices of symmetric $2-(n-1,\frac{n}{2}-1,\frac{n}{4}-1)$ designs and their corresponding complements can be such submatrices. The obtained Hadamard matrices are generator matrices to self-orthogonal codes over GF(2).

2. The Construction

Let $n \equiv 0 \ (mod\ 4)$. We construct a Hadamard matrix of order $4n$ from a given $2-(n-1,\frac{n}{2}-1,\frac{n}{4}-1)$ Hadamard design $\mathfrak{D}$. We consider the following structure of a Hadamard matrix of order $4n$ and denote it by H_{4n}.

$$H_{4n} := \left[\begin{array}{c|c|c|c|c}
1111 & 1111111\ldots & 1111111\ldots & 1111111\ldots & 1111111\ldots \\
1100 & 1111111\ldots & 1111111\ldots & 0000000\ldots & 0000000\ldots \\
1010 & 1111111\ldots & 0000000\ldots & 1111111\ldots & 0000000\ldots \\
1001 & 0000000\ldots & 1111111\ldots & 1111111\ldots & 0000000\ldots \\
\hline
1111 & & & & \\
\vdots & A_1 & A_2 & A_3 & A_4 \\
1111 & & & & \\
\hline
1100 & & & & \\
\vdots & B_1 & B_2 & B_3 & B_4 \\
1100 & & & & \\
\hline
1010 & & & & \\
\vdots & C_1 & C_2 & C_3 & C_4 \\
1010 & & & & \\
\hline
1001 & & & & \\
\vdots & D_1 & D_2 & D_3 & D_4 \\
1001 & & & &
\end{array}\right] \tag{1}$$

3. Properties of the $(n-1)\times(n-1)$ Block Matrices

To construct matrix (1), we need to find the block matrices A_1, A_2, A_3, A_4, B_1, B_2, B_3, B_4, C_1, C_2, C_3, C_4, D_1, D_2, D_3 and D_4. All of these are $(n-1)\times(n-1)$ matrices. We denote the *weight* (number of 1's entry) of a vector x as $wt(x)$ and the number of 1's intersection between any two row vectors x, y as $x * y$.

Lemma 3.1. *Row vectors of block matrices A_1, A_2, A_3, A_4, B_1, B_2, C_1, C_3, D_2 and D_3 are of weight $(\frac{n}{2}-1)$. Also, row vectors of block matrices B_3, B_4, C_2, C_4, D_1, and D_4 are of weight $\frac{n}{2}$.*

To construct matrix (1), we make use of the $(n-1)\times(n-1)$ incidence matrices of $\mathfrak{D}$ that is, block matrices A_1, A_2, A_3, A_4, B_1, B_2, C_1, C_3, D_2 and D_3 are incidence matrices of some $2-(n-1,\frac{n}{2}-1,\frac{n}{4}-1)$ Hadamard designs and, block matrices B_3, B_4, C_2, C_4, D_1, and D_4 are incidence matrices of some complements of the above designs. We can also consider incidence matrices from inequivalent $2-(n-1,\frac{n}{2}-1,\frac{n}{4}-1)$ Hadamard designs.
Let M be the $(4n-4)\times(4n-4)$ matrix obtained from deleting the first four rows and columns of matrix (1). Then

$$M \;:=\; \left[\begin{array}{c|c|c|c} A_1 & A_2 & A_3 & A_4 \\ B_1 & B_2 & B_3 & B_4 \\ C_1 & C_2 & C_3 & C_4 \\ D_1 & D_2 & D_3 & D_4 \end{array}\right] \qquad (2)$$

We define β_i $(i=1,2,3,4)$ as follows:

$\beta_1 = (\ A_1,\ A_2,\ A_3,\ A_4\ )$
$\beta_2 = (\ B_1,\ B_2,\ B_3,\ B_4\ )$
$\beta_3 = (\ C_1,\ C_2,\ C_3,\ C_4\ )$
$\beta_4 = (\ D_1,\ D_2,\ D_3,\ D_4\ )$

Let S be the set of $(n-1)\times(n-1)$ incidence matrices of some $2-(n-1,\frac{n}{2}-1,\frac{n}{4}-1)$ designs and M_i be an element of S. Denote M_i' as the incidence matrix of its corresponding complement and S' as the set of M_i'. We check some conditions of the block matrices in M to obtain different constructions of a Hadamard matrix using the given structure. Also, we determine the maximum number σ of distinct matrices from S which can altogether construct a Hadamard matrix. Observe that $\sigma\le 16$ since matrix M has 16 block matrices.

Lemma 3.2. *Let $A, B\in S$. Then for any vectors $x_A\in A$ and $y_B\in B$,*

$x_A * y_B = 0, 1, \ldots$ *or* $\frac{n}{2}-1$.

Lemma 3.3. *Let $A, B\in S$ and $0\le k\le \frac{n}{2}-1$. Then for any vectors $x_A\in A$ and $y_B\in B$,*

$x_{A'} * y_B = (\frac{n}{2}-1)-k$ *if and only if* $x_A * y_B = k$.

Lemma 3.4. *Let $A, B\in S$ and $0\le k\le \frac{n}{2}-1$. Then for any vectors $x_A\in A$ and $y_B\in B$,*

$x_{A'} * y_{B'} = k + 1$ *if and only if* $x_A * y_B = k$.

Let $A_1 = M_i$. Then we have the following possible values of β_1:

(i) If the A_i's $(i = 1, 2, 3, 4)$ are equal, then we have
1. $\beta_1 = (M_i, M_i, M_i, M_i)$.

(ii) If A_i $(i = 1, 2, 3, 4)$ have two different values, then we have
2. $\beta_1 = (M_i, M_i, M_j, M_j)$
3. $\beta_1 = (M_i, M_j, M_j, M_i)$
4. $\beta_1 = (M_i, M_j, M_i, M_j)$
5. $\beta_1 = (M_i, M_i, M_i, M_j)$
6. $\beta_1 = (M_i, M_i, M_j, M_i)$
7. $\beta_1 = (M_i, M_j, M_i, M_i)$
8. $\beta_1 = (M_i, M_j, M_j, M_j)$.

(iii) If $A_i (i = 1, 2, 3, 4)$ have three different values, then we have
9. $\beta_1 = (M_i, M_j, M_k, M_i)$
10. $\beta_1 = (M_i, M_j, M_k, M_k)$
11. $\beta_1 = (M_i, M_j, M_k, M_j)$
12. $\beta_1 = (M_i, M_i, M_j, M_k)$
13. $\beta_1 = (M_i, M_j, M_j, M_k)$
14. $\beta_1 = (M_i, M_j, M_i, M_k)$

(iv) If $A_i (i = 1, 2, 3, 4)$ have four different values, then we have
15. $\beta_1 = (M_i, M_j, M_k, M_l)$

The following is an algorithm in constructing the possible structures of M which would generate a Hadamard matrix of order $4n$:

(1) Consider the 15 possible values of β_1 above.
(2) For each case, generate the possible values of β_2. At this point, 15 sets of β_2 are generated.
(3) For every pair of β_1 and β_2, generate the possible values of β_3.
(4) For every triple of β_1, β_2 and β_3, generate the possible values of β_4.

Theorem 3.5. *There are* 149 *possible structures of* M *which would generate a Hadamard matrix of order* $4n$.

In finding values of $\beta_i (i = 1, 2, 3, 4)$, we use different variables and check all possibilities to find the maximum number of distinct block matrices which can altogether construct a Hadamard matrix of order $4n$. Hence we also have the following theorem:

Theorem 3.6. *The maximum number of distinct block matrices in matrix M which would construct a Hadamard matrix of order $4n$ is 4.*

4. The Hadamard Matrix of Order 32

We construct a Hadamard matrix of order 32 using the method in the previous section. $n = 32$ is the next length to be classified as $n \leq 28$ are completely classified. There are 26 matrices found in Seberry's homepage[15] and 6 matrices found in Sloane's page[14]. Araya, Harada and Kharaghani[1] also enumerated a number of them. It is known that there are at least 66,000 inequivalent Hadamard matrices of length 32[3].

The following are direct consequences of the results in the previous section:

(1) Let x_1 be the first row vector and let x, y be any distinct row vectors other than x_1. Then $x_1 * y = \frac{n}{2} = 16$ and $x * y = \frac{n}{4} = 8$ when $x \neq 1$.
(2) Row vectors of block matrices A_1, A_2, A_3, A_4, B_1, B_2, C_1, C_3, D_2 and D_3 are of weight 3. Also, row vectors of block matrices B_3, B_4, C_2, C_4, D_1, and D_4 are of weight 4.

We investigate other properties of the block matrices of a Hadamard matrix of order 32 by asking the question, "How many repetitions of row vectors are possible in constructing each block matrix?" The answer to this question gives the following result.

Proposition 4.1. 3 *repetitions of a vector in a block matrix is not possible, for block matrices A_i, B_i, C_i and $D_i (i = 1, 2, 3, 4)$.*

Hence, we are left with two remaining possibilities i.e., either a row vector in a block matrix can be repeated twice or each row vector is distinct.

5. Some Examples

We make use of the incidence matrices of the isomorphic $2-(7,3,1)$ designs and their respective complements, the $2-(7,4,2)$ designs. Note that these designs are unique and are self-dual[2]. There are 30 cosets of the $2-(7,3,1)$ designs and there are $(7!)^2/168$ incidence matrices. We use MAGMA in computing some Hadamard matrix examples. The following are some construction examples.

Example 5.1.

$$\begin{bmatrix} M_i & M_i & M_i & M_i \\ M_i & M_i & M_i' & M_i' \\ M_i & M_i' & M_i & M_i' \\ M_i' & M_i & M_i & M_i' \end{bmatrix}$$

If the construction used has one distinct block matrix, we obtain 1 *inequivalent Hadamard matrix of order* 32 *with automorphism group order equal to* 16515072.

Example 5.2.

$$\begin{bmatrix} M_i & M_i & M_i & M_i \\ M_j & M_j & M_j' & M_j' \\ M_i & M_i' & M_j & M_j' \\ M_i' & M_i & M_j & M_j' \end{bmatrix}$$

If the construction used has two distinct block matrices, we can obtain at most $\frac{7!^2}{168} \times \left(\frac{7!^2}{168} - 1\right)$ *Hadamard matrices of order* 32. *We have computed some Hadamard matrix examples from the above particular construction and obtained* 11 *different automorphism group orders namely:* 256, 768, 1024, 2048, 3072, 24576, 384, 512, 4096, 6144 *and* 65536.

Example 5.3.

$$\begin{bmatrix} M_i & M_i & M_i & M_i \\ M_j & M_j & M_j' & M_j' \\ M_k & M_k' & M_j & M_j' \\ M_k' & M_k & M_j & M_j' \end{bmatrix}$$

If the construction used has three distinct block matrices, we can obtain at most $\frac{7!^2}{168} \times \left(\frac{7!^2}{168} - 1\right) \times \left(\frac{7!^2}{168} - 2\right)$ *Hadamard matrices of order* 32. *We have computed some Hadamard matrix examples from the above particular construction and obtained* 13 *different automorphism group orders namely:* 256, 768, 1024, 2048, 3072, 24576, 64, 128, 192, 384, 512, 1536 *and* 4096.

Example 5.4.

$$\begin{bmatrix} M_i & M_j & M_k & M_l \\ M_i & M_j & M_k' & M_l' \\ M_i & M_j' & M_k & M_l' \\ M_i' & M_j & M_k & M_l' \end{bmatrix}$$

If the construction used has four distinct block matrices, we can obtain at most $\frac{7!^2}{168} \times \left(\frac{7!^2}{168} - 1\right) \times \left(\frac{7!^2}{168} - 2\right) \times \left(\frac{7!^2}{168} - 3\right)$ *Hadamard matrix of order* 32.

To classify the obtained Hadamard matrices of order 32, equivalence and automorphism group order must be considered. This can be done using MAGMA, too. Since computing requires a massive time, the total number of inequivalent Hadamard matrix of order 32 from the different obtained structures were not completely computed.

6. Ranks of a Hadamard Matrix of Order 32 over $GF(2)$ and Codes

Let H_n be a generator matrix of a linear binary $[n, k]$ code. The codes obtained from H_n when $n \equiv 0 \ (mod\ 8)$ is self-orthogonal and in particular, it yields self dual when $k = \frac{n}{2}$. The *2-rank* of H_n is the dimension of the $[n, k]$ code over $GF(2)$, and is written as $rank_2(H_n)$. This section enumerates $rank_2(H_n)$ of examples 5.1, 5.2, 5.3 and 5.4. Ranks of H_n were also computed using MAGMA.

We denote a Hadamard matrix of order 32 as H_{32}. From [2], $6 \leq rank_2(H_{32}) \leq 16$. $Rank_2(H_{32})$ in example 5.1 is 7; in examples 5.2 and 5.3 are 8, 9, 10, 11, 12 and 13. $Rank_2(H_{32}) = 14, 15, 16$ are not obtained from the computed examples but the author is hopeful to find examples of such ranks from the 149 different constructions. If H_{32} exists with $rank_2(H_{32}) = 16$ from any of our constructions, then we can also classify the $[32, 16]$ type II self dual codes obtained from Hadamard matrices with Hall sets[8].

7. Conclusions and Recommendations

In this paper, after checking the properties and conditions of the block matrices of matrix (1), we had come up with the following:

a. Construction of Hadamard matrices of order $4n$ if $n \equiv 0 \ (mod\ 4)$ and $2 - (n-1, \frac{n}{2} - 1, \frac{n}{4} - 1)$ Hadamard designs exist.
b. We were successful in enumerating all the possible constructions of a Hadamard matrix of order $4n$ using Kimura's structure, restricting the row vectors of each block matrix to be distinct and using the incidence matrices of a symmetric 2-design as block matrices of of such matrix.

For a Hadamard matrix of order 32 in particular, we also have come up with the following:

a. Some examples with their automorphism group orders and $Rank_2(H_{32})$ were computed,
b. 3 or more repetitions of a row vector in any of the 7×7 block matrices do not yield Hadamard matrix.
c. The possibility of constructing a Hadamard matrix using block matrices with vector/s repeated twice has not been explored.

Thus we are left with the following questions:

(1) Is there a possibility to construct a Hadamard matrix of order $4n$ using Kimura's structure if for any n, Hadamard $2-(n-1, \frac{n}{2}-1, \frac{n}{4}-1)$ design does not exist?
(2) If for $n = 8$, 3 or more repetitions of a row vector in any of the 7×7 block matrices of H_{32} do not yield Hadamard matrix, what would be the case for $n > 8$?
(3) Is there any relationship between the rank of a Hadamard matrix of order $4n$ ($n \geq 8$) and the constructions?
(4) Which of the constructions could generate Hadamard matrix of order $4n$of highest rank?
(5) Let H_{4n} be a Hadamard matrix of order $4n$. Is $rank_2(H_{4n}) = \frac{n}{2}$ possible in these constructions? If so, then we can also classify some Type II self dual codes from H_{4n}.

References

[1] M. Araya, M. Harada and H. Kharaghani, Some Hadamard Matrices of Order 32 and Their Binary Codes *(submitted).*

[2] E.F. Assmus, Jr. and J.D. Key, Designs and Their Codes, (*Cambridge University Press, Great Britain*, 1992).

[3] R. Craigen, Hadamard Matrices and Designs, *The CRC Handbook of Combinatorial Designs* , C.J. Colbourn and J.H. Dinitz(Eds.), CRC Press, Boca Raton 1996, 370–377.

[4] M.Hall, Jr.,Hadamard Matrices of Order 16, *J.P.L. Research Summary No.* **36–101** (1961) 21–26.

[5] M.Hall, Jr.,Hadamard Matrices of Order 20, *J.P.L. Technical Report No.* **32–761** (1965).

[6] N. Ito, J.S. Leon and J.Q. Longyear, Classification of $3-(24,12,5)$ Designs and 24-Dimensional Hadamard matrices, *J. Combin. Theory A* **31** (1981) 66–93.

[7] H. Kimura, New Hadamard matrices of Order 24, *Graphs Combin.* **5** (1989) 236–242.

[8] H. Kimura, Classification of Hadamard Matrices of Order 28, *Discrete Math.* **133** (1994) 171–180.

[9] Kimura, Hiroshi. (*private communication*)

[10] E.S. Lander, Symmetric Designs: An Algebraic Approach *London Mathematical Society Lecture Notes Series*, Cambridge University Press, Cambridge(1974).

[11] F.J. Macwilliams and N.J.A. Sloane, The Theory of Error-Correcting Codes, (*North-Holland, Amsterdam*, 1977).

[12] M. Ozeki, Hadamard Matrices and Type II Doubly-Even Error-Correcting codes *J. Combin. Theory A* **44** (1987) 274–287.

[13] E.M. Rains and N.J.A. Sloane, Self-Dual Codes, *Handbook of Coding Theory* , V.S. Pless and W.C. Huffman(Eds.), Elsevier Science B.V. 1998, 177-294.

[14] (http://www.research.att.com. njas/hadamard/index.html)

[15] (http://www.uow.edu.au/ jennie/hadamard/index.html)